REMARKS

As a preliminary matter, Applicant repeats and incorporates by reference herein those arguments previously presented in the Response filed June 9, 2008. Applicant respectfully requests that the Examiner reconsider those arguments, and withdraw the outstanding rejections of the claims. Section 707.07(f) of the MPEP places a burden upon the Examiner to first answer all meritorious arguments presented by Applicants in traversal of a rejection, before the rejection is repeated in a subsequent Office Action. In the present case, however, this burden has not been met.

For example, the Examiner asserts, in response to nearly every argument addressed in the "Response to Arguments" section of the outstanding Office Action, that "both references must be considered," and that "the entire references must be considered." Each of Applicant's previous meritorious arguments though, clearly argued against each of the cited references, alone and together. Moreover, Applicant has argued against the Examiner's reliance on the entirety of each of the references. Not once has the Examiner indicated that additional teachings – other than those already relied upon – from any reference somehow contradicts Applicant's meritorious arguments. It is inappropriate to merely dismiss an argument by asserting "the entire reference must be considered," but without indicating any single additional portion of the reference that supports the Examiner's reliance. Accordingly, the Office Action is nonresponsive in each instance where these assertions were made.

As another example, the outstanding Office Action inappropriately dismisses out of hand each of Applicant's previous arguments against the obviousness of combining references. The justification for such dismissal appears to be entirely based upon the Examiner's statement that "As per (sic) the KSR ruling prior art directed to the same subject matter can and should be combined." This statement represents a fundamental misunderstanding of both the holding of the cited U.S. Supreme Court case, as well as of patent law in general.

First, no such statement, or anything remotely similar, appears anywhere in the holding of *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398 (2007). Quite the contrary, the Supreme Court expressly forbade obviousness rejections based on unsupported conclusory statements: "Rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

conclusion of obviousness." 550 U.S. 398, 82 USPQ2d at 1396 (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006); see also MPEP 2143.01 (IV)) (emphasis added). The motivation to combine references must be based on clear evidence in the record, and such evidence has long been defined by the courts as that which is capable of objective review and rebuttal. In the present case, however, no such evidence has been cited by the Examiner.

Second, *KSR* did nothing to overturn the well established principle that still appears in Section 2143.01 of the MPEP, namely, that the mere fact that references "can be" combined will not sustain a rejection based on the obviousness of combining those references. The record must indicate where there was a clear teaching or suggestion to one of ordinary skill in the art to make the very combination proposed by the Examiner. *KSR* merely emphasized the existing law that states how the motivation may come from well-established principles in the art, as opposed to the text of the references themselves. Nevertheless, *KSR* clearly states that such motivation must still be supported by evidence on the record. In the present case, this burden has not been met. The mere statement that two references are in the same class and subclass does not even prove how the references *could be* combined, let alone that they should be combined. It should go without saying that many references in the same class and subclass can be mutually exclusive in their structures and/or methods. Accordingly, the outstanding Office Action is further non-responsive with respect to these meritorious arguments as well.

As a second preliminary matter, Applicant cannot understand the Examiner's statement "Third as shown in the Office Action '338 col. 2, lines 56-65 'an automated cooperative response' is interpreted to be equivalent is a process to network event" from page 8 of the outstanding Office Action. Clarification or withdrawal is requested.

Amendments to the Claims

Claims 1, 2 and 4-19 remain pending in the '852 Application.

Claims 1 is amended herein to clarify the cooperative nature of the cooperative agent cell by including the limitation that each agent communicates with at least one other agent within the cooperative agent cell. Support for this amendment can be found in at least paragraph [0019] of the specification and is shown in at least FIGs 3 and 4. Claim 1 is further amended to include the limitation that an initial assessment of the electronic network to determine normal activity is

made using one or more of the agents. Support for this amendment can be found in at least the abstract of the '852 Application.

Claim 18 is amended to correct a typographical error.

No new matter has been added to the claims by these amendments.

The following remarks attend to all issues presented in the Office Action dated September 09, 2008. Where used herein, numbered subtitles reflect the numbering of issues presented in the aforementioned the Office Action.

5. Claim Rejections – 35 U.S.C. 102

Claims 15-17 stand rejected under 35 U.S.C. 102(e) as being anticipated by '338.

Claim 15 recites a system for monitoring events within an electronic network, including:

a cooperative agent network having two or more agents, each agent installed within one component of the electronic network, the two or more agents forming at least one cooperative agent cell for collecting events from the electronic network, the cooperative agent network further comprising:

one or more event correlation engines, each event correlation engine being connected to the electronic network and having a receive event handler for receiving the events addressed to the event correlation engine; and

one or more event correlation modules, each of the event correlation modules having an event pattern that defines events of interest, each of the correlation modules receiving all events received by the event correlation engine, the event correlation module correlating the events of interest.

First, the Examiner is reminded that "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). MPEP 2143.03 (I). The Examiner is also reminded that in determining the scope of claims in patent applications the claims must be given their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004) (emphasis added), and that "the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach." *In re Cortright*, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999).

The Examiner's interpretation of the claimed agents as being equivalent to Rainforest agents is therefore unreasonable and incorrect according to these long-established principles of U.S. patent law. First, '338 discloses only that members are grouped based upon similar risk

profiles. The Rainforest agents do not form cooperative agent cells as recited by element (a) of claim 15. There is simply no disclosure within '338 of the Rainforest agents cooperating, as clearly defined in the present Specification. The assertion that a mere "grouping of agents" reads upon a cooperative agent cell is entirely erroneous. "Grouping," by itself, is not equivalent to "cooperating," according to not only the definitions within the present Specification, but also according to the plain and ordinary meaning of either term. Cooperation requires at least some interactivity toward a common purpose. Grouping two items, by itself, requires neither any interaction between the items, nor a common purpose. Furthermore, the Rainforests 12, 15 of '338 cannot be equivalent to an agent of claim 15 because neither Rainforest is installed within a component of an electronic network. For at least these reasons therefore, the rejection of claim 15 is deficient on its face, and should be withdrawn.

The rejection also fails to recognize differentiation between the correlation engine and the correlation modules, which are two separate and distinct elements of claim 15, as further shown in FIG. 5 of the '852 Application. The rejection, however, asserts that the event correlation engines of element (b) and the correlation modules of element (c) are both equivalent to the same "detection server" of '338. Despite the fact that Applicant has sufficiently demonstrated that neither of the correlation engine and the correlation modules are equivalent to the detection server of '338, under no reasonable interpretation – no matter how broad – could the same prior art element be equivalent to both separate and distinct features of the present claims. For at least these reasons as well, the rejection of claim 15 is further deficient, and should again be withdrawn.

Claims 16 and 17 depend from claim 15 and benefit from like arguments. These claims also have additional features that patentably distinguish over '338. For example, claim 16 features that the event correlation module is a simulated annealing correlator module. Simulated annealing is a known technique applied to the correlation module of claim 15. '338, however, fails to disclose simulated annealing, and therefore cannot anticipate claim 16. The rejection cites the application of threat-detection logic to parsed records and summing of threat values within '338 as allegedly anticipating simulated annealing. However, Applicants note for the record that one skilled in the art would have understood simulated annealing, as applied to correlation modules of claim 15, and in light of the accompanying disclosure, to be very different from the simple threat-detection and summed threat values of '338. See, for example,

http://www.nist.gov/dads/HTML/simulatedAnnealing.html, which gives one example of simulating annealing that negates the Examiner's particular interpretation.

Claim 17 features that the simulated annealing correlator further includes: (a) recorded events; (b) a simulated annealing correlator engine; (c) heuristics; and (d) a correlation threshold, wherein the simulated annealing correlator engine utilizes the heuristics and the correlation threshold to correlate the events received by the event correlation engine with the recorded events, the correlated events being added to the recorded events. '338 fails to disclose all of a simulated annealing correlator engine (as discussed immediately above), heuristics, and a correlation threshold. Although not previously known in the art according to the novel and nonobvious structure of the present claims, all of these terms were individually known to artisans of ordinary skill at the time of the invention, such that the interpretation of these terms in the rejection would be clearly negated as well.

For at least these reasons, '338 cannot anticipate either of claims 16 and 17. Reconsideration of claims 16 and 17 is respectfully requested.

7. Claim Rejections – 35 U.S.C. 103

Claims 1, 4, 6-9, and 18-19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,028,338 to Norris et al. (hereinafter, "'338") in view of U.S. Patent No. 7,096,499 to Munson (hereinafter "'499"). Applicants respectfully traverse this rejection for at least the reasons of record, and as follows. A *prima facie* case of obviousness has not been established.

The rejection appears to have failed to interpret either of the terms "agent" or "cooperative agent cell" of the '852 claims according to their clear definition in the present Specification. Each of the claims expressly require that the agents cooperate, that they communicate with one another, that they form a cooperative agent cell, that they monitor the electronic network for abnormal activity, and that they block the abnormal activity. All of these features are clearly defined in the Specification in such a way as to notably exclude the interpretations given to the different features cited from the prior art.

The Rainforest agents of '338 simply collect logs and send them to an external server. The Rainforest agents do not detect abnormal behavior, no matter how the elements are interpreted. The profile transducer of '499, on the other hand, simply accumulates module

frequencies of an instrumented computer program. The profile transducer does not detect any abnormal behavior either.

Moreover, the Rainforest agents of '338 do not form a cooperative agent cell. A mere grouping of two similar items, as discussed above, simply is not equivalent to cooperation between those two items. Similarly, '499 fails to disclose any cooperation between multiple profile transducers. Thus, neither the Rainforest agent of '338 nor the profile transducer of '499 detect abnormal behavior, and therefore neither, whether taken alone or together, can be considered equivalent to an agent of the '852 Application.

The claims of the '852 Application feature how the agents monitor the network for abnormal activity. Thus, these agents must clearly be able to detect such abnormal activity. (See at least paragraph [0021] of the '852 Application). In contrast, '338 states that "each member 20 is provided with its own *separate* instance of the Rainforest agent 13" (see '338 col. 4, lines 60-61), and that "[e]ven if a particular member 20 logs threatening activity, such as, for example, one hundred failed login attempts, each associated with a date/time stamp, over a relatively short period of time, ***the member 20 is unable to recognize the threat or take action on its own***, relying instead on the Alert Status 38 to tell it to take action." (See '338 col. 5, lines 32-37, emphasis added). '338 thus fails to teach or suggest a Rainforest agent detecting abnormal behavior, as required by the present claims. To further emphasize this deficiency in the prior art, it must be pointed out that the detection server 16 of '338 is not even installed on members of the electronic network, and thus could not monitor the network or take action when abnormal activity or a threat is detected. Thus, the Rainforest agents do not support the Examiner's reliance on the reference.

Additionally, and as previously argued, no actual motivation has been cited from either reference (nor from any well-known principle in the art) to support the proposed combination of '338 and '499. The only stated rationale for the combination (page 12 of the outstanding Office Action) is the quote from '499 that "It would be desirable to provide a real time intrusion detection paradigm that is applicable to monitoring almost any type of program." This simple reference to real time intrusion detection fails to overcome the clear deficiencies admitted by the Examiner from the '338 reference. The Examiner expressly admits that '338 fails to perform an initial assessment of the electronic network to determine normal activity. Whether or not such an initial assessment may be *useful* to real time intrusion detection, the two features are not

automatically related, as apparently presumed by the Examiner. More importantly, the citation to this portion of '499 fails to indicate how or why the reference should be combined with '338. Additional statements from '499 contradict the Examiner's conclusory assumptions regarding the proposed combination.

'499 expressly discloses that "[a] methodology presented herein reduces the dimensionality of the problem from a very large set of program instrumentation points representing small execution domains (modules or execution paths) whose activity is highly correlated to a much smaller set of virtual program domains *whose activity is substantially uncorrelated.*" (See '499 col. 4, lines 39-44, emphasis added). Because the profiled data in '499 is uncorrelated, it cannot read upon the claimed features of the present Application, namely, those features that unambiguously establish how correlation is used to identify abnormal activity. Accordingly, not only does the rejection fail to establish the required rationale for combining the references, '499 actually teaches away from the proposed combination.

Individual claims in the rejection are addressed as follows:

Regarding Independent Claim 1: Amended claim 1 recites a method of protecting an electronic network, including:

(a) installing two or more agents within components of the electronic network;

(b) logically connecting the agents into one or more cooperative agent cells, each agent communicating with at least one other agent within the cooperative agent cell;

(c) performing an initial assessment of the electronic network, using one or more of the agents, to determine normal activity;

(d) monitoring the electronic network for abnormal activity using the agents; and

(e) protecting the electronic network by blocking the abnormal activity using the agents.

Neither '338 nor '499 teach or suggest to monitor an electronic network. The rejection only asserts that '338 (and not even '499) discloses the monitoring of *log and audit records*. Log and audit records are not necessarily equivalent to an electronic network. Whether or not the features may be related or utilized together, they are nevertheless not the same. The Examiner is reminded that "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). MPEP 2143.03 (I). The electronic network of claim 1 is clearly defined within the present

Specification, and not in a way that would render it reasonably equivalent to only log and audit records, as cited from '338.

Applicants further note that the rejection appears to confuse the term "Rainforest agent" and "Rainforest" with respect to '338. These two terms are clearly distinct within the reference:

> As illustrated, the system 10 is used to monitor one or more domains (hereinafter referred to as "***Rainforests***") 12, and broadly comprises one or more instances of a ***Rainforest Agent*** 13; one or more log servers 14; one or more detection servers 16; and one or more profile servers 18. Each Rainforest 12 is a domain defined as a logical grouping of a plurality of members 20, wherein the logical grouping may be based on a variety of factors or member characteristics, including, for example, the members' nature, use, value, and risk tolerance. The members 20 may be any devices or edge devices or objects, including, for example, servers, mainframes, personal computers, firewalls, and routers, and ***need not necessarily be on the same network or in direct contact with or even geographically near one another***. '338 col. 3, lines 31-45 (emphasis added).

Members (and hence, Rainforest agents) of the Rainforest could not form a cooperative agent cell, according to the claims of the present Application, when the members are not in direct communication with one another. As discussed above and previously, '338 simply does not disclose the claimed cooperation of Rainforest agents. A Rainforest agent does not include all of the functionality of the Rainforest, and the Rainforest itself is not equivalent to one of its many agents, or more particularly, a cooperative agent network as in the present Application.

Each cooperative agent cell in the present claims may perform monitoring and strategic investigation of suspected activity by mapping agents 24 and attack agents 26. (See at least paragraph [0020]). A cooperative agent cell is well defined to include agents that cooperate to perform monitoring and strategic investigation.

In the interests of expediting prosecution, step (b) of claim 1 has been amended herein to clarify that <u>each agent communicates with at least one other agent within the cooperative agent cell.</u> The Rainforest agents of '338, however, do not form any such cooperative agent cell, and each Rainforest agent is not disclosed to communicate with at least one other Rainforest agent in such a cooperative agent cell as recited by step (b). The Examiner has only asserted that Rainforest agents may communicate with each other, but not that such agents <u>additionally</u> form a cooperative cell.

Step (c) of claim 1 features that one or more of the claimed agents performs an initial assessment of the electronic network to determine normal activity. As discussed above, the

Examiner asserts that the profile transducer of '499 can be interpreted to be equivalent to an agent. However, Applicant again points out that the *profile transducer* of '499 does not perform an initial assessment of an electronic network to determine normal activity. The profile transducer of '499 merely accumulates module or execution path frequencies of an instrumented computer program. The cited text section clearly indicates that the transducer is merely a "functional component" of the anomaly detection methodology (col. 5, lines 28-29), and that only its output is sent for analysis. (Col. 5, lines 43-44). The transducer itself does not make any initial assessment. The assessment *of* the transducer is performed by an execution profile comparator. (Col. 4, lines 65-66).

In response to Applicant's arguments that "neither '338 nor '499 disclose monitoring an electronic network for abnormal activity using agents," the Examiner now asserts that "Munson teaches that the agents signal the detection server which detects, i.e., monitors for threatening or otherwise suspicious activity i.e., abnormal activity." However, Munson does not disclose any such detection server. The detection server was cited by the Examiner from within **'338**, and thus Munson cannot signal a detection server from a completely different reference, as erroneously asserted.

As discussed above, the Office Action fails to specifically address Applicant's argument that neither '338 nor '499 disclose monitoring an electronic network for abnormal activity using agents. As previously noted, the "detection" in '338 occurs within a detection server that is *external* to the protected domain. The Examiner asserts that the instrumented software program, such as email Internet browsers, readily recognize network links or network activities. The mere *possibility* of recognition, however, is not the same as the affirmatively-claimed monitoring. Applicants again point out that '499 only monitors a computer program's *reaction* to network events, which is not the same as monitoring the network itself, since computer programs, such as email client and a browser, receive network messages addressed only to the computer program, and makes only selectively programmed responses thereto. The present claims do not recite monitoring of program behavior; rather, the claims recite that each cooperative agent cell monitors the electronic network to detect abnormal behavior.

Thus, neither '338 nor '499 discloses monitoring an electronic network for abnormal behavior, and using the agents, as recited by step (d) of claim 1. As taught by at least paragraph [0020] of the '852 Application, agents form one or more cooperative agent cells to perform

monitoring and strategic investigation of suspected activity by mapping agents and attack agents. That is, in step (d) of claim 1, the agents monitor the electronic network for abnormal activity; these agents do not simply collect data for external processing, but also determine abnormal activity. As noted above, the Rainforest agents of '338 simply send log and audit information to the external detection server. The Rainforest agents do not themselves determine whether activity is abnormal.

Furthermore, the log information of '338 that is collected by the Rainforest agents and sent to the log server is disclosed as containing information related to use and attempted use of the members. (See '338 col. 5, lines 15-17). There is no disclosure within '338 of actually monitoring the electronic network for abnormal activity. There is no disclosure or suggestion that the log information is itself the network activity.

As featured in claim 1, agents are logically connected into one or more agent cells, they perform an initial assessment of the electronic network, they monitor the electronic network for abnormal activity, and they protect the electronic network by blocking the abnormal activity. The Rainforest agents of '338 and the profile transducer of '499 cannot perform any of these functions, let alone all of them, and therefore these prior art elements cannot be equivalent to the featured agents of claim 1.

For at least these reasons and the reasons previously presented, '338 and '499, even when combined, cannot render claim 1 obvious. Reconsideration of claim 1 is respectfully requested.

Claims 4 and 6-9 depend from claim 1 and benefit from like arguments. These claims also have additional features that patentably distinguish over '338 and '499. For example, claim 4 features that the step of installing further includes: establishing bidirectional communication protocols for agent communication within the cooperative agent cells; delegating one or more agents in the cooperative agent cells to have bidirectional communication with another delegated agent; and establishing bidirectional communication protocols for each delegated agent to communicate with another delegated agent. None of the cited references, whether taken alone or together, teach or suggest all of these features.

Claim 6 recites that the step of logically connecting further includes self-organizing at least one of the agents into each of the cooperative agent cells. As previously argued, Rainforest agents each have a Rainforest configuration file that tells the Rainforest agent to which domain

the member belongs, to which log server to send log and audit records, and which profile server to periodically query for updates to a security profile. (See '338 col. 2, lines 9-15). Rainforest agents are thus organized only *by the configuration file*, and not by themselves. The Examiner asserts that the text "some or all peripheral devices in a network advertise their availability to the network via a non-routable protocol," allegedly requires self-organizing. This assertion is clearly erroneous. A mere advertisement does not require self-organization. For example, a printer may "advertize" its availability to print within a network, but such an advertisement clearly would not amount to self-organization with other printers, which may be in the same network, into a printer cell. Organization requires a comparative order. Advertising, by itself, requires no such thing.

Claim 7 features that the step of establishing further includes communicating via at least one covert communication protocol. The Examiner asserts that "using the broadest reasonable interpretation of a cover [sic] protocol is equivalent to a 'special broadcast message via a non-routable protocol.'" The mere fact that a broadcast message is "special," however, has nothing to do with whether the message is covert. As defined by dictionary.com, for example, "covert" means: concealed, secret, or disguised. The special broadcast of '338 clearly fails to meet this plain meaning of the term. In fact, '338 even states that Netbios is an example of the 'non-routable protocol,' and Netbios is well known in the art to not be a "covert" protocol.

Claim 8 features that the step of performing an initial assessment includes mapping systems, communication ports, and attached devices of the electronic network, and establishing normal activity of the systems, communication ports, and attached devices. The Examiner asserts, however, that "using the broadest reasonable interpretation an initial assessment comprising mapping, communication ports and attached devices is equivalent to a probe that monitors hardware addresses." This assertion is clearly erroneous for several reasons.

First, the probe of '499 monitors hardware *addresses* of running software, and not the hardware itself. Second, it is the step of performing an initial assessment of the electronic network to determine normal activity in the claim that maps systems, communication ports and attached devices of the electronic network. '499, on the other hand, states (col. 5, lines 30-35) "The transducer obtains signals from an instrumented software system 301 and computes activity measures for these signals .... The actual software signals may be obtained either from instrumented code (software probes) or directly from a hardware address bus (a hardware probe)." The *hardware address bus* is not, by itself, equivalent to an electronic network. The

rejection fails to answer to Applicant's previous meritorious arguments on these issues. Merely repeating the rejection is not an answer, as clearly indicated by Section 707.07(f) of the MPEP.

Claim 9 features that the step of monitoring includes: (a) non-destructively intercepting communications on the electronic network; (b) collecting events from the intercepted communications; and (c) determining if the events indicate abnormal activity. Again, the rejection is non-responsive to the meritorious arguments addressing the deficiencies of the prior art with respect to these claim features. The Office Action provides no clarification how "non-destructively intercepting communication on the electronic network" is somehow taught or suggested by only the "collecting and analyzing that is done in '338." As previously pointed out, '338 makes no disclosure of non-destructively intercepting communications on an electronic network.

For at least these reasons, '338 and '499, alone or in combination (or with any other reference of record), cannot render claims 4 or 6-9 obvious. Reconsideration of claims 4 and 6-9 is therefore respectfully requested.

Regarding Independent Claim 18: Amended claim 18 recites a method of pattern recognition, including:

(a) performing an initial assessment of the electronic network;

(b) collecting electronic network events;

(c) sampling the electronic network events with one or more event correlation engines;

(d) passing sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine;

(e) comparing events in each of the event correlator modules by sampling the events, determining if any of the events matches an event pattern, and, if there is a match, creating a new event announcing the match and passing the new event to the associated event correlation engine for electronic network distribution; and

(f) determining patterns in events using a simulated annealing correlator, determining if the pattern is important, and, if so, creating a new event announcing the important pattern and passing the new event to the associated event correlation engine for network distribution.

The rejection erroneously asserts that the multiple servers of '338 are somehow equivalent to the multiple correlation engines of claim 18. '338, however, fails to anywhere teach or suggest that detection servers 16 implement correlation engines. '338 simply states that detection server 16 monitors and parses log and audit records for signs of threatening or

otherwise suspicious activity. (See col. 5, lines 26-28). Nowhere does the reference teach or suggest correlation, let alone multiple correlation engines, as erroneously asserted. Applicants do not claim to have invented correlation, a process that is separately known in the art, but instead the novel and nonobvious use of correlation within an event correlation engine.

Correlation is simply not equivalent to "reviewing the received data," as erroneously asserted. According to the plain meaning of the term, "correlation" is defined as "the degree to which two or more attributes or measurements on the same group of elements show a tendency to vary together." (www.dictionary.com). Merely reviewing data will not, by itself, indicate such tendencies or variances. Obviousness is not established by mere possibilities or probabilities. There must be some clear teaching or suggestion of the claimed limitations. In the present case, however, the rejection of claim18 appears to be based solely on the *possibility* that the claimed features *could be* implemented into the prior art. As discussed above, Section 2143.01 forbids rejections based only on the fact that a reference *can be* modified.

The Office Action further asserts that "using the broadest reasonable interpretation multiple correlation engines are equivalent to the multiple servers that are defined within the multiple Rainforest agents." Rainforest agents in '338, however, are not taught or suggested to include multiple (or even single) servers. The rejection, as noted previously and above, confuses Rainforest agents with Rainforests.

As previously argued, the detection server of '338 is external to the protected domain and does not process events collected from the electronic network. In contrast, the present Application describes and claims that the correlation for identifying abnormal behavior is applied to network events by one or more agents. These features are not equivalent to "reviewing the received data in order to detect abnormal behavior," as erroneously asserted. Such interpretation is not reasonable in light of the specification that clearly defines the use of correlation within a correlation engine to detect abnormal behavior.

'338 states that "[t]he threat-detection logic may be simple or complex, depending on a number of considerations, including the nature and value of the members 20. For example, in one possible threat-detection logic scheme, suspicious behaviors are associated with threat values, and when the sum of threat values for the domain exceed the Threshold Value 40, a threat is determined to exist." (Col. 3 line 66, through col. 4 line 6). Although '338 states that suspicious behaviors are *associated* with threat values, '338 fails to teach or suggest how such

suspicious behaviors are identified. The Examiner appears to suggest that a detection server that parses through records with threat-detection logic uses "heuristics." This assumption though, is purely a matter of the Examiner's own conclusory opinion, as '338 makes no disclosure or suggestion of using heuristics at all. *KSR* clearly forbids such conclusory statements to justify an obviousness rejection.

For at least these reasons, '338 and '499, alone or in combination, cannot render claim 18 obvious. Reconsideration of claim 18 is respectfully requested.

Claim 19 depends from claim 18 and benefits from like argument. However, claim 19 has additional features that patentably distinguish over '338 and '499. For example, claim 19 features that the step of sampling further comprises sampling all of, or less than all of, the electronic network events. The Office Action entirely fails to address any of Applicant's arguments regarding the deficiencies of the cited art with respect to claim 19, and is thus further nonresponsive. As previously argued, neither '338 nor '499 disclose sampling electronic network events, and therefore the proposed combination could not teach or suggest sampling all of, or less than all of, the electronic network events.

Reconsideration of claim 19 is therefore also respectfully requested.

Claims 2 and 5 stand rejected under 35 U.S.C. 103(a) as being unpatentable over '338 in view of '499 and in further view of U.S. Patent Number 7,007,301 to Crosbie et al. (hereinafter '301). Applicants respectfully traverses this rejection for at least the reasons of record, those discussed above, and as follows. Claims 2 and 5 depend from claim 1 and benefit from the same arguments presented above with respect to the rejection of claim 1 based only on '338 and '499.

Additionally, claim 2 features that the step of installing comprises the step of installing a type 2 super peer agent for authenticating, authorizing and reauthorizing the agents. Claim 5 recites that the step of installing further includes broadcasting a request for agents to submit to authentication, and authenticating submitted agents.

The Examiner erroneously asserts that Crosbie somehow discloses a type 2 super peer agent. As defined within the present Specification though, a type 2 super peer agent "runs on a dedicated host computer (e.g., component 14(E), FIG. 1A), and may be denoted as an 'agent authorization and configuration hub.'" (Paragraph [0028]). Although the Examiner dismisses Applicant's arguments against the rejection of this claim, the Office Action provides no further

explanation or argument to challenge Applicant's meritorious arguments. The Office Action merely asserts that "Applicant cannot place limitations from the specification into the claims." Applicant respectfully point out to the Examiner though, that claim 2 recites "installing a type 2 super peer agent for authenticating, authorizing and reauthorizing the agents," and that the Examiner is required to interpret this claim limitation in light of the Specification. The Examiner may not simply dismiss Applicant's argument that SSL is a communication protocol, and is not equivalent to the type 2 super peer agent as the term is defined in the present Specification. Applicants have not otherwise argued in favor of any limitations that do not already appear the claims. The claims already feature the limitations of authenticating, authorizing, and reauthorizing.

Further, the shortfall of '338 and '499 in rendering claim 1 obvious is also not overcome by '301. For example, '301 fails to disclose performing an initial assessment of the electronic network using the agents to determine normal activity and monitoring the electronic network for abnormal activity using the agents.

For at least these reasons, '308, '499, and '301 cannot render claims 2 and 5 obvious. Reconsideration of claims 2 and 5 is therefore also respectfully requested.

In response to Applicant's traversal of the rejection of claims 10-14, the Office Action is further nonresponsive for simply stating disagreement with the arguments, but without providing any additional reasons or explanation for the disagreement. Applicant's meritorious arguments in favor of claims 10-14 thus remain unchallenged on the record as a matter of law.

Nevertheless, the Examiner is reminded that "Office personnel should consider all rebuttal arguments and evidence presented by applicants." See, e.g., *Soni*, 54 F.3d at 750, 34 USPQ2d at 1687. The Examiner is required to consider all such evidence of nonobviousness when assessing patentability. *In re Soni*, 54 F.3d 746, 750 (Fed. Cir. 1995); *In re Sernaker*, 702 F.2d 989, 996 (Fed. Cir. 1983). In the present case, however, the Examiner has failed to meet this burden of giving meaningful consideration to Applicant's meritorious arguments traversing the rejections.

Addressing these claims individually:

Claim 10 stands rejected under 35 U.S.C. 103(a) as being unpatentable over '338 in view of '499, in further view of U.S. Patent No. 7,085,936 to Moran (hereinafter '936). Applicants

respectfully traverse this rejection for at least the reasons of record, those discussed above, and as follows. A *prima facie* case of obviousness has not been established against claim 10.

Depending from claim 1, claim 10 benefits from arguments presented above for claim 1, included here by reference. Furthermore, claim 10 features that the step of protecting comprises one or more of:

(a) luring a malicious agent that causes abnormal activity into a false appearance of success;

(b) planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent;

(c) isolating electronic network components which have been compromised by the malicious agent;

(d) attacking the malicious agent;

(e) formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network;

(f) installing patches to eliminate vulnerabilities in the electronic network;

(g) reassessing the electronic network to detect abnormal operations; and

(h) investigating abnormal operations of the electronic network.

As argued previously and above, neither '338 nor '499 teaches or suggests using agents to monitor an electronic network. The Examiner correctly acknowledges that '338 and '499 do not explicitly teach at least steps (a) and (b) of claim 10. The rejection then relies upon '936 for allegedly teaching steps (c), (d), (e), (f), (g), and (h), asserting that '936 teaches "the system includes a trap system create a virtual cage in col. 7, lines 42-51." Respectfully, Applicants point out that these assertions are still erroneous. As previously argued, '936 fails to disclose cooperative agents for intrusion detection, and therefore fails to overcome the shortfall of '338 and '499 in rendering claim 1 obvious.

Step (c) of claim 10 features isolating electronic network components which have been compromised by the malicious agent. The '936 patent is silent as to isolating compromised components, the reference's *modus operandi* being to divert the attacker into a trap. Step (d) of present claim 10 features attacking the malicious agent. '936 is silent about attacking the malicious agent as well, given its use of the trap. Step (e) of claim 10 features formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network. '936 is also

silent as to formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network. As disclosed at col. 12, lines 14-18, '936 relies upon a *system administrator* to block future attacks. Step (f) of claim 10 features installing patches to eliminate vulnerabilities in the electronic network. '936, however, again relies upon the *system administrator* to block attacks, and therefore '936 could not install patches. Step (g) of claim 10 features reassessing the electronic network to detect abnormal operations. '936 fails to disclose that the electronic network is reassessed to detect abnormal operations.

For at least these reasons, '338, '499, and '936, alone or in combination, cannot render claim 10 obvious.

Claims 11-13 stand rejected under 35 U.S.C. 103(a) as being unpatentable over '338 in view if '499 in further view of U.S. Patent No. 7,058,968 to Rowland et al. (hereinafter '968). Applicants respectfully traverse for at least the reasons of record, those above, and as follows. Claims 11-13 depend from claim 1 (via claim 3) and benefit from the arguments presented above with respect to the rejection of claim 1. Neither '338 nor '499 disclose using agents to monitor an electronic network, and '968 clearly fails to overcome this deficiency of '338 and '499.

Claim 11 additionally features promoting one of the agents in each of the cooperative agent cells to a cell delegate. The rejection asserts that col. 4, lines 44-67, of '968 somehow teaches or suggests that the architecture of the system is design to allow modularity, which allows for the roles to be reversed. This assertion fails to provide any rationale for how such role reversal within a cell of like agents results in promotion of one agent to a cell delegate. '968 simply fails to disclose cooperative agent cells, or that one agent within the cooperative agent cell is promoted to a cell delegate. As described by paragraph [0026] of '852, "active agent 34 is promoted to cell delegate 36 if it is the first authenticated and authorized agent of cooperative agent cell 28." The agent promotion of claim 11 is not defined as a "role reversal," and it cannot be equivalent to the role reversal of '968, since role reversal requires that a cell delegate already exists.

Claim 12 features promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent, authenticating new agents with the type 1 super peer agent, and communicating between the cooperative agent cells and a command and control console via the

cell delegate to protect the network from malicious activity. The cited references clearly fail to teach or suggest all of these features.

Again, the rejection cites only col. 4, lines 44-67 of '968 as allegedly teaching that the architecture of the system is designed to allow modularity, which allows for the roles to be reversed. As discussed immediately above, '968 fails to disclose any cooperative agent cells or promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent. As described by paragraph [0027] of '852, "[a]ctive agent 34 and cell delegate 36 may be promoted to T1SPA 38, as necessary, provided that the host component 14 has sufficient resources to support T1SPA 38." The agent promotion of claim 12 thus is also not a role reversal, nor could it be equivalent to the role reversal of '968, since such role reversal requires that a type 1 super peer agent already exists.

Furthermore, '968 fails to disclose communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity. As argued above, '968 fails to disclose cooperative agent cells and cell delegates. Accordingly, the rejection of claim 12 individually should also be reconsidered and withdrawn.

Claim 13 features that agents and cooperative agent cells are configured for independent and collaborative investigation of the electronic network, isolation of compromised components of the electronic network, and defense of the electronic network. Once again, only col. 4, lines 44-67 of '968 is cited as allegedly teaching or suggesting such features. The cited role reversal of '968 is still inapplicable to claim 13 as well, and for the same reasons discussed above with respect to claims 11 and 12.

For at least these reasons, '388, '499 and '968, alone or in combination, cannot render claims 11, 12 and 13 obvious. Reconsideration of claims 11, 12 and 13 is respectfully requested.

Regarding Independent Claim 14: Claim 14 stands rejected under 35 U.S.C 103(a) as being unpatentable over '338 in view of '499 in further view of '936. Applicants respectfully disagree.

As previously argued, Applicants believe the combination of '338 and '499 to be nonobvious if not impossible in view of the different operation of each of '338 and '499.

Independent claim 14 recites a system for protecting an electronic network, comprising:

(a) a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate;

(b) a communications protocol within each cooperative agent cell, for (a) communicating between agents of the cooperative agent cell, and (b) communicating with cell delegates external to the cooperative agent cell;

(c) means for determining normal activity levels of the electronic network;

(d) means for detecting malicious activity;

(e) means for isolating compromised components of the electronic network;

(f) means for counter-intelligence to reveal the origin of the malicious activity;

(g) means for repairing damage caused by the malicious activity;

(h) means for determining vulnerabilities in the current protection provided by the plurality of agents; and

(i) means for improving protection to resist future attack on the electronic network.

Element (a) of claim 14 features a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate. That is, a group of agents form a cooperative agent cell wherein these agents cooperate with one another and promote one agent to be the delegate for the cooperative agent cell. The cell delegate collects and filters data from the other agents within its cooperative agent cell and passes the data to a collection point in the cooperative agent network. (See '852 Application paragraph [0026], for example). The rejection cites only col. 1, lines 54-67 of '338 as allegedly teaching or suggesting element (a) of claim 14. However, no features of element (a) have actually been identified within the cited portion of '388, and therefore the rejection is still deficient. The Examiner does not answer Applicant's meritorious arguments traversing the rejection merely by stating that the whole reference should be considered. If the Examiner is relying on a portion of the reference other than what is cited by the Examiner, the Examiner should identify such portions on the record. Applicant submits though, that no uncited portions of the reference read upon the present claims either.

The cited passage of '338 clearly fails to disclose any of: cooperative agents; a cooperative agent cell; and a cell delegate. The Rainforest agent of '338 does not cooperate; it does not form a cooperative agent cell; and it does not represent a cell delegate. Applicants submit that each of the Rainforest agents operate independently to send log and audit records of a

member to a designated log server. (See '338 col. 2, lines 7-15). The log server is not an agent, nor is it a cell delegate. '499 and '936 fail to resolve these clear deficiencies of '338.

Element (b) of claim 14 features a communications protocol within each cooperative agent cell, for communicating between agents of the cooperative agent cell, and communicating with cell delegates external to the cooperative agent cell. Since '338 fails to disclose cooperating agents, cooperative agent cells, and cell delegates, '338 cannot disclose a protocol for communicating therebetween. As discussed above, the Rainforest agents of '338 do not communicate with one another within the Rainforest. '499 and '936 again fail to resolve these deficiencies from '338.

Element (c) of claim 14 features means for determining normal activity levels of the electronic network. That is, the agents monitor network activity during normal operation of the electronic network to determine levels of normal network activity. (See paragraph [0020] of the '852 Application, for example). The Examiner correctly acknowledges that these features of element (c) are not taught by '338. The Examiner relies only upon '499 for allegedly teaching or suggesting "that normal profiles data are initially established by a calibration process that is implemented by running the program in a calibration mode in col. 5, lines 5-15." However, the '499 calibration process is performed for a single running program, and makes no assessment of actual electronic network activity, as featured by element (c). This deficiency of both '338 and '499 is not resolved by '936.

Element (d) of claim 14 features means for detecting malicious activity. As described by paragraph [0020] of the '852 Application, each cooperative agent cell performs monitoring and strategic investigation of suspect activity by mapping agents 24 and/or attach agents 26. That is, within each cooperative agent cell, agents operate to detect malicious activity by investigating suspect network activity and identifying abnormal activity levels within the electronic network. The rejection relies on col. 3, line 63, through col. 4 line 10, of '338 as somehow showing means for detecting malicious activity. However, the detection server 16 of '338 is not an agent cooperating within a cooperative agent cell. The detection server 16 is a dedicated computer system that is external to, but connected to, the networked members. The Examiner has asserted that the individual *members* are equivalent to the claimed agents, and not computer system connected to the network. The operation of '338 is therefore clearly different from that of the

'852 Application. Nothing has been cited from '499 or '936 to resolve this clear deficiency from '338.

Element (e) of claim 14 features means for isolating compromised components of the electronic network. That is, the compromised component is isolated to prevent further malicious activity. The rejection cites only col. 7, lines 42-51 of '936 as allegedly teaching these features of element (e), but this reliance on the reference is misplaced. The trap system 210 of '936 is separate from the protected network and into which an intruder attempting to gain access to the protected system is diverted. This trap system 210 is not a compromised component. For at least this reason, element (e) cannot be rendered obvious by any combination of '338, '499, and '936.

Element (f) of claim 14 features means for counter-intelligence to reveal the origin of the malicious activity. The rejection cites only col. 4, lines 45-51 of '338 as somehow teaching or suggesting these features of element (f). This reliance is also misplaced because the cited passage only discloses that Rainforest agents broadcast an alert and instruct routers and firewalls to block traffic from particular networks. Counter-intelligence to reveal the origin of the malicious activity is not taught or suggested by '338, '499, or '936.

Element (g) of claim 14 features means for repairing damage caused by the malicious activity. Element (h) features means for determining vulnerabilities in the current protection provided by the plurality of agents. Element (i) features means for improving protection to resist future attack on the electronic network. The rejection cites only col. 12, lines 9-29 of '936 as somehow teaching or suggesting these features. Although '936 does disclose information to a system administrator indicating configuration problems that may fit with the factors that made the attack possible, there is no disclosure in the reference of a means for repairing the damage caused by the malicious activity, as required by element (g), or of means for improving protection to resist future attack on the electronic network, as required by element (i). In particular, '936 relies upon the judgment and action of the *system administrator* in repairing and improving protection of the network, and thus does not perform such tasks automatically.

For at least these reasons, '338, '499, and '936, alone or in combination, cannot render claim 14 obvious. Reconsideration of claim 14 is respectfully requested.

CONCLUSION

In view of the above Remarks, Applicant submits that all issues raised in the Office Action dated September 09, 2008 have been addressed. All pending claims are submitted to be allowable. Applicants respectfully request a Notice of Allowance for all of claims 1, 2, and 4-19.

The Examiner is, as always, encouraged to telephone Applicant's attorney, Curtis A. Vock, at (720) 931-3011 to discuss the amendments presented herein, or any outstanding issues regarding the '852 Application.

The Commissioner is authorized to charge $555 for three month extension of time and $405 for the Request for Continued Examination to deposit account No. 12-0600. It is believed that no additional fees are due with this response, however, if any fee is deemed necessary in connection with this Amendment and Response, the Commissioner is authorized to please charge all such fees to Deposit Account No. 12-0600.

Respectfully submitted,

LATHROP & GAGE LLP

Date: 10 Feb. 2009

By: Heather Perrin

Heather F. Perrin, Reg. No. 52,884
4845 Pearl East Circle, Suite 201
Boulder, Colorado 80301
Tele: (720) 931-3033
Fax: (720) 931-3001